Migrating from RedHat to SUSE Linux Enterprise Server 10 Administration Workbook

COURSE 3068

Novell Training Services

www.novell.com

AUTHORIZED COURSEWARE

Part # 103-000297-001
Version 1

Novell®

Proprietary Statement

Novell, Inc.
1800 South Novell Place
Provo, UT 84606-2399

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to revise this publication and to make changes in its content at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software at any time, without obligation to notify any person or entity of such changes.

This Novell Training Manual is published solely to instruct students in the use of Novell networking software. Although third-party application software packages are used in Novell training courses, this is for demonstration purposes only and shall not constitute an endorsement of any of these software applications.

Further, Novell, Inc. does not represent itself as having any particular expertise in these application software packages and any use by students of the same shall be done at the students' own risk.

Software Piracy

Throughout the world, unauthorized duplication of software is subject to both criminal and civil penalties.

If you know of illegal copying of software, contact your local Software Antipiracy Hotline.

For the Hotline number for your area, access Novell's World Wide Web page at http://www.novell.com and look for the piracy page under "Programs."

Or, contact Novell's anti-piracy headquarters in the U.S. at 800-PIRATES (747-2837) or 801-861-7101.

Trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell, Inc. Trademarks

Novell, the Novell logo, NetWare, BorderManager, ConsoleOne, DirXML, GroupWise, iChain, ManageWise, NDPS, NDS, NetMail, Novell Directory Services, Novell iFolder, Novell SecretStore, Ximian, Ximian Evolution and ZENworks are registered trademarks; CDE, Certified Directory Engineer and CNE are registered service marks; eDirectory, Evolution, exteNd, exteNd Composer, exteNd Directory, exteNd Workbench, Mono, NIMS, NLM, NMAS, Novell Certificate Server, Novell Client, Novell Cluster Services, Novell Distributed Print Services, Novell Internet Messaging System, Novell Storage Services, Nsure, Nsure Resources, Nterprise, Nterprise Branch Office, Red Carpet and Red Carpet Enterprise are trademarks; and Certified Novell Administrator, CNA, Certified Novell Engineer, Certified Novell Instructor, CNI, Master CNE, Master CNI, MCNE, MCNI, Novell Education Academic Partner, NEAP, Ngage, Novell Online Training Provider, NOTP and Novell Technical Services are service marks of Novell, Inc. in the United States and other countries. SUSE is a registered trademark of SUSE LINUX GmbH, a Novell company. For more information on Novell trademarks, please visit http://www.novell.com/company/legal/trademarks/tmlist.html.

Other Trademarks

Adaptec is a registered trademark of Adaptec, Inc. AMD is a trademark of Advanced Micro Devices. AppleShare and AppleTalk are registered trademarks of Apple Computer, Inc. ARCserv is a registered trademark of Cheyenne Software, Inc. Btrieve is a registered trademark of Pervasive Software, Inc. EtherTalk is a registered trademark of Apple Computer, Inc. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds. LocalTalk is a registered trademark of Apple Computer, Inc. Lotus Notes is a registered trademark of Lotus Development Corporation. Macintosh is a registered trademark of Apple Computer, Inc. Netscape Communicator is a trademark of Netscape Communications Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. Pentium is a registered trademark of Intel Corporation. Solaris is a registered trademark of Sun Microsystems, Inc. The Norton AntiVirus is a trademark of Symantec Corporation. TokenTalk is a registered trademark of Apple Computer, Inc. Tru64 is a trademark of Digital Equipment Corp. UnitedLinux is a registered trademark of UnitedLinux. UNIX is a registered trademark of the Open Group. WebSphere is a trademark of International Business Machines Corporation. Windows and Windows NT are registered trademarks of Microsoft Corporation.

All other third-party trademarks are the property of their respective owners.

Contents

SECTION 5 Manage System Initialization

SECTION 6 Configure Mail and Web Services

SECTION 7 AppArmor

SECTION 8 Manage Virtualization with Xen

SECTION 9 iSCSI

SECTION 10 Cluster File Systems

Introduction

This workbook is designed to help you practice the skills associated with *Migrating from RedHat to SUSE Linux Enterprise Server 10* (Course 3068) objectives.

By covering the administrative details specific to SUSE Linux Enterprise Server 10, this course prepares you to take the Novell Certified Linux Professional 10 (Novell CLP 10) certification practicum test—provided you already have the general Linux knowledge covered in the courses *SUSE Linux Enterprise Server 10 Fundamentals* (Course 3071), *SUSE Linux Enterprise Server 10 Administration* (Course 3072), and *SUSE Linux Enterprise Server 10 Advanced Administration* (Course 3073).

The *Migrating from RedHat to SUSE Linux Enterprise Server 10* Course DVD contains an image of a SUSE Linux Enterprise Server 10 installation that you can use with the *Migrating from RedHat to SUSE Linux Enterprise Server 10* Workbook outside the classroom to practice the skills you need to take the Novell CLP 10 Practicum exam.

A VMware image without installed operating system is also provided. You can use it to install SUSE Linux Enterprise Server 10 as described in the exercise for Section 1.

Instructions for setting up a self-study environment are in the directory setup on the Student DVD.

Exercise Conventions

When working through an exercise, you will see conventions that indicate information you need to enter that is specific to your server.

The following describes the most common conventions:

- ***italicized/bolded text***. This is a reference to your unique situation, such as the host name of your server.

  For example, if the host name of your server is DA50, and you see the following,

  ***hostname*.digitalairlines.com**

  you would enter

  DA50.digitalairlines.com

- **10.0.0.*xx***. This is the IP address that is assigned to your SUSE Linux Enterprise Server 10 server.

  For example, if your IP address is 10.0.0.50, and you see the following

  10.0.0.*xx*

  you would enter

  10.0.0.50

- **Select.** The word *select* is used in exercise steps to indicate a variety of actions including clicking a button on the interface and selecting a menu item.

- **Enter and Type.** The words *enter* and *type* have distinct meanings.

  The word *enter* means to type text in a field or at a command line and press the Enter key when necessary. The word *type* means to type text without pressing the Enter key.

  If you are directed to type a value, make sure you do not press the Enter key or you might activate a process that you are not ready to start.

SECTION 1 Install SUSE Linux Enterprise Server 10

In this section of the workbook, you learn how to do the following:

- "Install SUSE Linux Enterprise Server 10" on 1-2

  In this exercise, you install SUSE Linux Enterprise Server 10.

Exercise 1-1 Install SUSE Linux Enterprise Server 10

In this exercise, you install SUSE Linux Enterprise Server 10. Use the following specifications as a guideline:

- One partition with 1 GB for swap.
- One partition with 6 GB for / (there should be space left on the hard disk to add partitions in later exercises).
- Use default software patterns, add the C/C++ Compiler and Tools pattern
- root password: novell

  (As ***novell*** is, of course, not adequate as a root password in production, you could use a different one; however, the exercises in this manual refers to ***novell*** as the root password.)
- Use a fixed IP address; the instructor will let you know which one to use:
  - IP address:
  - Network mask: **255.255.255.0**
  - Host name:
  - Domain name: **digitalairlines.com**
  - Name server: **10.0.0.254**
  - Default gateway: **10.0.0.254**

  (In case you are doing this exercise in self-study with no other students in the network, use 10.0.0.10 as IP address and da10 as hostname.)
- Use local authentication; create a user account geeko, password: novell.
- Skip the online update

Detailed Steps to Complete this Exercise:

- Part I: Boot From the Installation Media
- Part II: Configure the Partitions for Your Hard Drive
- Part III: Configure the Installed Server

Part I: Boot From the Installation Media

To boot from the installatin media, do the following:

1. Turn on the computer.
2. Insert *SUSE Linux Enterprise Server 10 DVD* into the DVD drive.
3. (Conditional) If your computer does not boot from the DVD drive, reboot the computer by selecting the **Reset** button or by pressing **Ctrl+Alt+Del**.

   Adjust the BIOS settings so that the DVD drive is the first boot device and reboot the computer.
4. When the GRUB installation screen appears, select **Installation** with the arrow keys and press **Enter**.
5. From the language selection dialog, select ***your language***; then select **Accept**.

Although you can select any available language, the exercises in this manual are written for English US.

6. When YaST displays the **Novell Software License Agreement**, select **Yes, I Agree to the License Agreement** and then Next.
7. When the installation mode dialog appears, select **New Installation**; then select **Next**.
8. Select your time zone in the **Clock and Time Zone** dialog. Select UTC and adjust the time to your current time, if needed.

When done, select **Next**. An Installation Settings proposal dialog appears.

9. Select **Keyboard Layout**; Select ***your keyboard layout***; then select **Accept**.

   You are returned to the Installation Proposal dialog.

Part II: Configure the Partitions for Your Hard Drive

1. Change the partitioning settings by selecting **Partitioning**.
2. Select **Create Custom Partition Setup**; then select **Next.**
3. Select **Custom Partitioning -- for experts;** then select **Next.**
4. Delete existing partitions:
   a. From the Expert Partitioner dialog, check for any existing partitions in the partition list.
   b. If there are partitions, select the ***hard disk entry*** of the corresponding partitions (such as **hda** or **hdc**).
   c. Delete all existing partitions on the selected hard disk by selecting **Delete**.
   d. When you are asked to confirm the deletion, select **Yes**.
   e. (Conditional) If there is more than one hard disk containing partitions in the system, repeat Steps **b**, **c**, and **d** until only the hard disk entries are left in the list.
5. Create a swap partition:
   a. From the partition list, select the ***hard drive entry***; then select **Create**.

      If you have more than one hard disk, select the larger disk.
   b. Select **Primary partition**; then select **OK**.
   c. In the End field of the size settings enter **+1GB**.
   d. From the File system drop-down list, select **Swap**.
   e. Add the swap partition by selecting **OK**.

6. Create the root partition:
   a. Select the same hard disk you used for the swap partition; then select **Create**.
   b. Select **Primary partition**; then select **OK**.
   c. In the End field of the size settings enter **+6GB**.
   d. Make sure that the following options are set:
      - **Reiser** should be selected from the File system drop-down list.
      - **/** should be selected from the Mount Point drop-down list.
   e. Add the root partition by selecting **OK**.
7. Confirm the partitioning setup and return to the installation proposal by selecting **Finish**.
8. From the Installation Settings Overview, select **Accept**.
9. From the confirmation dialog, select **Install**.
10. (Conditional) If you are usinge the CD set instead of the DVD, YaST asks you to change CDs during the installation process and the server might reboot when the software from the first CD is installed.

    Insert the requested CDs and select **OK**.

Part III: Configure the Installed Server

1. When presented with the **Hostname and Domain Name** dialog, enter the ***hostname*** in the **Hostname** field and ***digitalairlines.com*** in the **Domain Name** field.
2. Remove the selection in front of Change Hostname via DHCP; then select **Next**.
3. You are presented with the **Password for the System Administrator "root"** dialog. Enter **novell** in the **Password for root User** and the **Confirm Password** fields.
4. Continue by selecting **Next**.

You are warned that the password is too simple.

5. Continue by selecting **Yes**.

   You are warned that you are using only lowercase letters.

6. Continue by selecting **Yes**.

7. In the **Network Configuration** proposal, under **Firewall** select **enabled**. The entry will change to **Firewall is disabled**.

8. From the Network Configuration proposal, select **Network Interfaces**.

9. Select the first detected network card and select **Edit**.

10. Select **Static Address Setup**.

11. In the **IP Address** field, enter ***your IP address***.

12. In the **Subnet Mask** field, enter **255.255.255.0**.

13. Configure the host name and name server:

    a. Select **Hostname and Name Server**.

    b. You hostname and domain name should already be filled in correctly; if not, enter your ***hostname*** and the domain name **digitalairlines.com**.

    c. In case **Update Name Servers and Search List via DHCP** is selected, remove the selection by clicking on it.

    d. In the Name Server 1 field, enter the **10.0.0.254** of the name server.

    e. Return to the Network setup dialog by selecting **OK**.

14. Configure routing:

    a. Select **Routing**.

    b. In the Default Gateway field, enter **10.0.0.254**.

    c. Return to the Network setup dialog by selecting **OK**.

15. Return to the Network Configuration dialog by selecting **Next**.

16. Continue with the installation by selecting **Next**; then select **Next** once more.

17. From the Test Internet Connection dialog, select **No, Skip This Test**; then select **Next.**
18. From the **Service Configuration** dialog, accept the default settings by selecting **Next**.
19. For the User Authentication Method, select **Local (/etc/passwd)**; then select **Next**.
20. Add a user:
    a. User's Full Name: **Geeko Novell**
    b. User Login: **geeko**
    c. Password: **novell**
    d. Confirm password: **novell**
    e. Create the user by selecting **Next**; confirm the dialogs about a too simple password and an all lower case password with **Yes**.
21. From the **Release Notes** dialog, select **Next**.
22. In the **Hardware Configuration** dialog, review the settings suggested under **Graphics Cards**. On those that are incorrect, select the respective entry and correct it in the dialog that opens up.
23. Once the settings are correct, in the Hardware configuration dialog select **Next**.
24. Complete the installation process by selecting **Finish**.

(End of Exercise)

SECTION 2 YaST

In this section of the workbook, you learn how to do the following:

- "Get to Know YaST" on 2-2

  In this exercise, you learn how to use the different user interfaces of YaST and how to start some YaST modules.

- "Install New Software" on 2-5

  In this exercise, you install another software package that is available on the SUSE Linux Enterprise Server 10 installation media.

- "Manage User Accounts with YaST" on 2-7

  In this exercise, you create and remove an user account with the YaST user management module.

- "Configure the Password Security Settings" on 2-9

  In this exercise, you practice changing different security settings.

Exercise 2-1 Get to Know YaST

In this exercise, you learn how to use the different user interfaces of YaST and how to start some YaST modules. In part I, you start the graphical user interface of YaST. In part II, you view the file /proc/version with the YaST system log module. In part III, you to set the time. Repeat part I and II with the ncurses user interface of YaST in part IV and V.

To use YaST, do the following:

- Part I: Start YaST
- Part II: View the Content of a System Log File
- Part III: Change Time and Date
- Part IV: Start the ncurses Interface of YaST
- Part II: View the Content of a System Log File
- Part VI: Exit YaST

Part I: Start YaST

To start YaST, do the following:

1. From the GNOME desktop, open the main menu.
2. Select **More Applications**.
3. Enter **ya** into the Filter text box.
4. Select the **YaST** icon to start YaST.
5. Enter the root password **novell** in the appearing dialog; then select **Continue** or press Enter.

   The YaST Control Center appears.

Part II: View the Content of a System Log File

To view the content of a system log file, do the following:

1. Select **Miscellaneous > View System Log**.

2. From the top drop-down list, select **/proc/version**.
3. Close the log window by selecting **OK**.

Part III: Change Time and Date

To change time and date, do the following:

1. Select **System > Date and Time**.
2. Select **Change**.
3. Enter the current time (such as **08:00:00**) and the current date (such as **27/04/2006**).
4. Select **Apply**.
5. Select **Accept**.

Part IV: Start the ncurses Interface of YaST

To start the ncurses interface of YaST, do the following:

1. Switch to the first virtual terminal by pressing **Crtl+Alt+F1**.
2. Log in as **root** with a password of **novell**.
3. View a list of the available YaST modules by entering **yast -l**.
4. Enter **yast** to start the ncurses interface of YaST.

Part V: View the Content of a System Log File

To view the content of a system log file, do the following:

1. Press **cursor-down** until **Miscellaneous** is highlighted in the left frame and press **Enter**.
2. Press **cursor-down** until **View System Log** is highlighted in the right frame and press **Enter**.
3. Press **cursor-down** until **/proc/version** is selected and press **Enter**.

4. Press Tab twice to highlight **OK** and press **Enter**.

Part VI: Exit YaST

To exit YaST, do the following:

1. Press **Alt+Q** to select **Quit**.
2. Log out by entering
   exit
3. Switch back to the graphical interface by pressing **Crtl+Alt+F7**.
4. Close the YaST window.

(End of Exercise)

Exercise 2-2 Install New Software

In this exercise, you install another software package that is available on the SUSE Linux Enterprise Server 10 installation media. It is called *locate* and it is needed in one of the following sections.

To install new software, do the following:

- Part I: Start YaST
- Part II: Look for a Software Package
- Part II: Install a Software Package and Finish

Part I: Start YaST

To start YaST, do the following:

1. From the GNOME desktop, open the main menu.
2. Select **More Applications**.
3. Enter **ya** into the Filter text box.
4. Select the **YaST** icon to start YaST.
5. Enter the root password **novell** in the appearing dialog; then select **Continue** or press **Enter**.
6. The YaST Control Center appears.

Part II: Look for a Software Package

To look for a software package, do the following:

1. From the YaST Control Center, select **Software > Software Management**.
2. From the Filter drop-down list, select **Search**.
3. In the Search textbox enter **locate**; select **Search**.

Part II: Install a Software Package and Finish

To install a software package and finish, do the following:

1. From the right side of the window, select the package **findutils-locate**.
2. Select **Accept**.
3. (Conditional) If requested by YaST, insert the appropriate *SUSE Linux Enterprise Server 10 DVD*; then select **OK**.
4. When asked to install or remove more packages, select **No**.
5. Close the YaST Control Center by selecting **Close**.
6. (Conditional) If you installed from DVD, remove the DVD from your drive.

(End of Exercise)

Exercise 2-3 Manage User Accounts with YaST

In this exercise, you create and remove a user account with the YaST user management module. In part I, you create a new account labeled “tux” for the user “Tux Penguin” with the password of “novell”. In part II, you log in as user tux. In part III, you open the file /etc/passwd and look for the entries for geeko and tux. In part IV, you log in as geeko and remove tux’s account.

To manage user accounts with YaST, do the following:

- Part I: Create a New User Account with YaST
- Part II: Log In as New User
- Part III: View the passwd File

Part I: Create a New User Account with YaST

To create a new user account with YaST, do the following:

1. From the GNOME desktop, select **Applications > System > YaST**; then enter a password of **novell** and select **Continue**.

   The YaST Control Center appears.

2. From the YaST Control Center, select **Security and Users > User Management**.
3. Add a new user by selecting **Add**.
4. Enter the following information:
   - User’s Full Name: **Tux Penguin**
   - Username: **tux**
   - Password: **novell**
   - Confirm Password: **novell**
5. When you finish, select **Accept**.
6. Confirm the password warning by selecting **Yes**.
7. Save the new settings by selecting **Finish**.
8. Close the YaST window.

Part II: Log In as New User

To log in as the new user, do the following:

1. From the bottom panel, log out by selecting **Desktop > Log Out**.
2. In the log out dialog, select **OK**.

   X Window is restarted and the GUI login screen appears.
3. In the Username field enter **tux** and press **Enter**.
4. In the Password field enter **novell** and press **Enter**.
5. Close or cancel any displayed dialogs.

Part III: View the passwd File

To view the passwd file, do the following:

1. Start the Nautilus file manager by double-clicking the **tux's Home** icon on the desktop.

   The content of tux's home directory is displayed.
2. Browse to the directory **/home**.

   Notice there are directories for users tux and geeko.
3. Browse to the directory **/etc**.
4. Select the file **passwd**.

   Notice the entries for users tux and geeko at the end of the file.
5. Close all windows.

(End of Exercise)

Exercise 2-4 Configure the Password Security Settings

In this exercise, you practice changing different security settings. Change the default behavior when the keys Ctrl+Alt+Del are pressed to halting the machine. Also change the encryption from blowfish to MD5. Use the YaST Local Security module to do the above.

Detailed Steps to Complete this Exercise:

1. Open a terminal window.
2. Check the setting for the Ctrl+Alt+Del keystroke in the file /etc/inittab by entering **grep ctrlaltdel /etc/inittab.**

   Note the current setting:

3. Start **YaST** and select **Security and Users > Local Security**.

   The Local Security Configuration dialog appears.
4. Make sure **Custom Settings** is selected; then select **Next**.

   The Password Settings dialog appears.
5. From the Password Encryption Method drop-down list, select **MD5**.
6. Continue by selecting **Next**.

   The Boot Settings dialog appears.
7. From the Interpretation of Ctrl + Alt + Del drop-down list, select **Halt**.
8. Continue by selecting **Next**.

   The Login Settings dialog appears.
9. Accept the default settings by selecting **Next**.

   The Adding User dialog appears.

10. Accept the default settings by selecting **Next**.

    The Miscellaneous Settings dialog appears.

11. Accept the default settings and configure the system for the new settings by selecting **Finish**.

12. To test the change, you must first activate the new configuration by rebooting the system or by entering (as root) **init q** (reload the /etc/inittab file) in a terminal window.

    a. From the terminal window, **su -** to root (password **novell**).

    b. Reload the file /etc/inittab by entering **init q**.

13. Verify that the Ctrl+Alt+Del setting has changed by entering **grep ctrlaltdel /etc/inittab**.

    Notice that the setting is now “shutdown -h” instead of what you noted in Step 2.

14. Test this setting by pressing **Ctrl+Alt+F2**; then press **Ctrl+Alt+Del**.

    The system shuts down instead of restarting.

15. Turn on your computer and log in to the Gnome desktop as **geeko**.

16. (Optional) Use the YaST Security settings module to change the default for **Ctrl+Alt+Del** back to restart.

(End of Exercise)

SECTION 3 Network Configuration

In this section of the workbook, you learn how to do the following:

- "Manage the Network Configuration Information from YaST" on 3-2

  In this exercise you change all the network configuration information into static values.

- "Configure the Network Connection Manually" on 3-6

  In this exercise, you learn how to configure the network manually.

Exercise 3-1 Manage the Network Configuration Information from YaST

Up to now, your system got all network configuration information via DHCP. In this exercise you change all the important information into static values.

Use the **ip** command to find out which ip address you are currently using. Also note your current hostname. Then change the network configuration to static IP addresses, using the values you found. Use 10.0.0.254 as default gateway and also as address of the name server.

To manage the network configuration information from YaST, do the following:

- Part I: Get your IP Number and Hostname
- Part II: Start the YaST Network Configuration Module
- Part III: Enter a Static IP Address and Subnet Mask
- Part IV: Change your Hostname
- Part V: Enter a DNS Server
- Part VI: Enter a Default Gateway
- Part VII: Activate new Settings and Finish

Part I: Get your IP Number and Hostname

To get your IP number and hostname, do the following:

1. From the GNOME desktop, open the main menu.
2. Select **More Applications**.
3. Enter **term** into the Filter text box.
4. Select the **Gnome Terminal** icon to start a terminal emulation.
5. Enter **/sbin/ip address show** to record the following information for your SUSE Linux Enterprise Server 10 server:
   - IP address:
   - Hostname:

6. Close the terminal window.

Part II: Start the YaST Network Configuration Module

To start the network configuration module of YaST, do the following:

1. From the GNOME desktop, open the main menu.
2. Select **More Applications**.
3. Enter **ya** into the Filter text box.
4. Select the **YaST** icon to start YaST.
5. Enter the root password **novell** in the appearing dialog; then select **Continue** or press Enter.

   The YaST Control Center appears.
6. Start the network card module by selecting **Network Devices > Network Card**.

Part III: Enter a Static IP Address and Subnet Mask

To enter a static IP address and subnet mask, do the following:

1. Make sure that **Traditional Method with ifup** is selected and select **Next**.

   Your network card is listed in the upper table.
2. Make sure ***your network card*** is selected; then select **Edit**.
3. Make sure that the **Address** tab is activated.
4. Switch the setup by selecting **Static address setup**.
5. In the IP Address field, enter the ***IP address*** from Part I.
6. In the Subnet mask field, enter **255.255.255.0**.

Part IV: Change your Hostname

To change your hostname, do the following:

1. Select **Host name and name server**.
2. (Conditional) If a dialog appears indicating that the **resolv.conf** files has been temporarily modified, continue by selecting **Modify**.
3. In the Hostname field, enter the ***hostname*** from Part I.
4. In the Domain Name field, enter **digitalairlines.com**.

Part V: Enter a DNS Server

To enter a DNS server, do the following:

1. In the Name Server 1 field, enter the IP address of your DNS server (**10.0.0.254**).
2. If there are values in the other Name Server text fields, remove them.
3. In the Domain Search field, enter **digitalairlines.com**.
4. If there are values in the other Domain Search text fields, remove them.
5. Select **OK**.

Part VI: Enter a Default Gateway

To enter a default gateway, do the following:

1. Select **Routing**.
2. In the Default Gateway field, enter the IP address of your Internet gateway (**10.0.0.254**).
3. Select **OK**.

Part VII: Activate new Settings and Finish

To activate new settings and finish, do the following:

1. Select **Next**.
2. Select **Next**.
3. Close the YaST Control Center.
4. To test your network connection, start the web browser Firefox and try to call http://www.novell.com.

(End of Exercise)

Exercise 3-2 Configure the Network Connection Manually

The purpose of this exercise is to familiarize you with manually configuring the network.

In the first part, using the command ip, find out the current settings for IP address, routes, mac address, and the file used to store the hardware configuration of the network card in /etc/sysconfig/hardware/ and the configuration options in that file.

In the second part, using YaST, delete the current network configuration.

In the third part, using the ip command, set up the network manually. As only the command ip is used, this configuration is not permanent.

In the fourth part, recreate the file in /etc/sysconfig/hardware/ noted in part I using an editor, as well as the files /etc/sysconfig/network/ifcfg-eth-id-***MAC-address*** and /etc/sysconfig/network/routes. Reboot the computer and test the network to see if the network is set up correctly after a reboot.

Detailed Steps to Complete this Exercise:

- Part I: Note the Current Network Configuration
- Part II: Delete the Current Network Setup with YaST
- Part III: Configure the Network Manually
- Part IV: Save the Network Connection to Interface and Hardware Configuration Files

Part I: Note the Current Network Configuration

To note the current network configuration, do the following:

1. On the graphical desktop, open a terminal window and **su -** to root (password **novell**).
2. Enter **ip address show eth0** (depending on the setup you might have to use eth1 instead of eth0).
3. Find the line starting with **inet**, and record the ***IP address*** with the ***subnet mask*** displayed in that line:
   - **IP address:**
   - **Subnet mask:**
4. Enter **ip route show**.
5. Find the line starting with **default** and record the ***gateway IP address*** of the gateway:
   - **Gateway IP address:**
6. Enter **ip link show eth0**.
7. Find the line starting with **link/ether** and record the ***MAC address*** of the network card:
   - **MAC address:**
8. Change to the /etc/sysconfig/hardware directory by entering the following:

   cd /etc/sysconfig/hardware
9. Enter **ls -al**; then look for one of the following files (depending on your hardware configuration):
   - **hwcfg-id-*PCI_address***

     or
   - **hwcfg-bus-pci-*PCI_address***
10. Record the name of the file:

Note: If there are several files with the above pattern, enter **lspci** in a terminal window. The output shows the PCI addresses of PCI hardware components in your computer.

11. Display the contents of the file by entering one of the following:
    - **cat hwcfg-id-*PCI_address***

      or
    - **cat hwcfg-bus-pci-*PCI_address***
12. Record the following parameters:
    - **MODULE=**
    - **MODULE_OPTIONS=**
    - **STARTMODE=**

    You use these parameters and the hwcfg filename in Part IV to manually create the file.

Part II: Delete the Current Network Setup with YaST

To delete the current network setup with YaST, do the following:

1. Start **YaST** and select **Network Devices > Network Card**.
2. Select **Traditional Method with ifup.**
3. Select the ***network card***; then select **Delete**.
4. Select **Next**.
5. From the terminal window (as root), enter **rm /etc/sysconfig/network/routes**.
6. Verify that the network connection is not working any more by entering **ping 10.0.0.254**.
7. Enter **ip address show**.

   Note that the device eth0 is not up anymore or no longer listed.

Part III: Configure the Network Manually

To configure the network manually, do the following:

1. To initialize the device eth0 again, enter in the terminal window:

   hwup bus-pci-*PCI_address*

   You noted the PCI address in Part I, Step 10. The command should look similar to the following:
   hwup bus-pci-000\:02\00.0

2. Enter the following command:

   ip address add *your_IP_address*/24 brd + dev eth0

3. To activate the network device, enter **ip link set eth0 up**.

4. To set the default route enter the following:

   ip route add default via *gateway_IP_address*

5. Verify that the network connection is working again by entering **ping www.novell.com**.

Part IV: Save the Network Connection to Interface and Hardware Configuration Files

To save the network connection to interface and hardware configuration files, do the following:

1. From the terminal window, change to the directory **/etc/sysconfig/network**.

2. Make a copy of the network configuration template by entering the following:

   cp ifcfg.template ifcfg-eth-id-*MAC_address*

3. Open the copied file (**ifcfg-eth-id-*MAC_address***) with the **vi** editor.

4. Find the following options and enter the indicated values:

   - STARTMODE=**'auto'**
   - BOOTPROTO=**'static'**

- IPADDR='***your_IP_address*/24'**
- NETMASK=**'255.255.255.0'**
- BROADCAST=**'10.0.0.255'**

5. Save the file and exit vi (**:wq**).
6. Change to the directory **/etc/sysconfig/hardware**.
7. Create one of the following files with **vi**:
   - **hwcfg-id-*PCI_address***

     or

   - **hwcfg-bus-pci-*PCI_address***
8. Enter the parameters you recorded in the last step of Part I of this exercise.
9. When you finish, save the file and exit the editor.
10. Change to the directory **/etc/sysconfig/network**.
11. Create a new file with vi called **routes**.
12. Add the following line to the file:

    default *default_gateway_IP_address* - -
13. Save the file and exit vi.
14. Reboot your system (**init 6**) and log in as **geeko** with a password of **novell**.
15. From a terminal window (as root), verify that the network configuration is loaded correctly by entering the following commands:

    ip address show eth0
    ip route show
16. Verify that the network connection is working properly by entering the following commands:

    ping 10.0.0.254

If the network configuration fails to work properly, and your configuration files are created correctly, use the YaST Network Card module to delete the currently configured network card. Then restart the Network Card module and reconfigure the network card with the proper settings.

(End of Exercise)

SECTION 4 Manage the Linux File System

In this section of the workbook, you learn how to do the following:

- "Configure Partitions on Your Hard Drive" on 4-2

  In this exercise, you practice creating partitions and file systems on them with YaST and **fdisk**. You also use command line tools to create file systems.

- "Manage File Systems from the Command Line" on 4-9

  In this exercise you practice to manage file systems from the command line.

- "Create Logical Volumes" on 4-13

  In this exercise, you learn how to administer LVM with YaST.

Exercise 4-1 Configure Partitions on Your Hard Drive

In this exercise, you practice creating partitions and file systems on them using YaST and fdisk. You also use command line tools to create file systems.

In the first part of this exercise, use YaST to create the following partitions and file systems:

- An extended partition using the remaining disk space.
- One logical partition with a size of 500 MB, an ext2 file system, and a mountpoint of /apps.
- One logical partition with a size of 1 GB, a Reiser file system, and a mountpoint of /srv.

In the second part of this exercise, use fdisk to create the following partitions:

- One partition of the partition type Win95/FAT32 with a size of 500 MB
- Two partitions with the partition type Linux and a size of 1 GB and 2 GB, respectively

After this exercise, there should still be space left on the hard disk to create additional partitions. If disk space is limited, use smaller values for the partitions than those given here to make sure there is empty space for later exercises.

In the third part, you create file systems on the partitions you created in Part II, using the applicable options for mkfs:

- Create a FAT32 file system on /dev/hda7 (or /dev/sda7, depending on your hardware).
- Create an ext2 file system on /dev/hda8 (or /dev/sda8, depending on your hardware).
- Create a Reiser file system with a file system size of 625 MB on /dev/hda9 (or /dev/sda9, depending on your hardware).

Detailed Steps to Complete this Exercise:

- Part I: Create Partitions and File Systems with YaST
- Part II: Partition Manually with fdisk

Part I: Create Partitions and File Systems with YaST

To create partitions and file systems with YaST, do the following:

1. Open a terminal window, **su -** to root (password novell), and enter **yast2 disk**

   A warning message appears.

2. Continue by selecting **Yes**.

   After a few moments the Expert Partitioner dialog appears.

3. If there is no extended partition yet, create an extended partition with YaST:
   a. Create a new partition by selecting **Create**.
   b. Make sure **Extended Partition** is selected; then select **OK**.

      A **Create an Extended Partition** dialog appears.

   c. Make sure that the values in the fields for first and last cylinder of the extended partition comprise the whole remaining disk space. Then select **OK**.

      You are returned to the Expert Partitioner dialog, with the new partition listed as a new entry for your hard disk.

4. Create a new ext2 partition with YaST:
   a. Create a new partition by selecting **Create**.
   b. Configure a new logical partition by entering or selecting the following:
      - File system: **Ext2**
      - End (cylinder): **+500M**
      - Mount Point: **/apps**

   c. When you finish, confirm the partition definition by selecting **OK**.

You are returned to the Expert Partitioner dialog where the new partition is added to the list.

The asterisk (*) after the mount point signifies that the file system is not mounted right now (see explanation in the help text to the left).

5. Create a partition for the directory /srv:

   a. Select the same hard disk as before; then select **Create**.

   b. Configure a new logical partition by entering or selecting the following:

      - File system: **Reiser**
      - End (cylinder): **+1G**
      - Mount Point: **/srv**

   c. Add the /srv partition by selecting **OK**.

      You are returned to the Expert Partitioner dialog where the new partition is added to the list.

6. Add the new partitions to the hard drive by selecting **Apply**.

   A dialog appears asking if you really want to execute the changes.

   Continue by selecting **Finish**.

   This executes the changes and closes the Expert Partitioner dialog. If you select **Apply** instead of **Finish**, the changes are executed and you are returned to the Expert Partitioner dialog.

7. Verify creation of the new partition for /apps:

   a. In the terminal window where you are logged in as root, verify that the new partition is mounted by entering **mount**.

      You should see the following line:

      ```
      /dev/hda5 on /apps type ext2 (rw)
      ```

   b. Verify that the appropriate entry was added to the /etc/fstab for the new partition by entering the following:

      cat /etc/fstab

      You should see the following:

```
/dev/hda5   /apps   ext2   acl,user_xattr  1 2
```

This entry makes sure that when the system boots, the new file system is mounted.

8. The current content of the directory /srv is no longer visible, as it is used as mount point for the partition /dev/hda6 (or /dev/sda6, depending on your hardware). To copy the content to the new partition, do the following:

   a. Unmount /dev/hda6 (or /dev/sda6, depending on your hardware) by entering:

      umount /srv

   b. Mount the partition /dev/hda6 (or /dev/sda6, depending on your hardware) under /mnt by entering:

      mount /dev/hda6 /mnt

   c. Move the content of /srv to /mnt :

      mv /srv/* /mnt

   d. Umount /mnt and mount /dev/hda6 (or /dev/sda6, depending on your hardware) again, using the entries in /etc/fstab:

      umount /mnt
      mount -a

   e. Verify that the files you moved are available again under /srv by entering

      ls /srv/

Part II: Partition Manually with fdisk

To partition manually with fdisk, do the following:

1. From the command line, start the utility fdisk on the first IDE hard disk on your server by entering **fdisk /dev/hda** (if your computer uses SATA or SCSI disks, enter **fdisk /dev/sda**). Depending on the number of cylinders on your disk a message is displayed that the number of cylinders is above 1024, which might cause problems under certain circumstances.
2. View the current partition table in fdisk by entering **p**.

Notice that there are 5 partitions (hda1, hda2, hda3, hda5 and hda6).

3. Create a new 500MB Win95 FAT32 logical partition as the next partition in the extended partition by doing the following:
   a. Create a new partition by entering **n**.
   b. Enter **l** (lower case L) for logical.
   c. Accept the default first cylinder by pressing **Enter**.
   d. Indicate the partition size by entering **+500M**.
   e. Change the partition type to Win95 FAT32 by entering **t** (for type, the highest partition number from the range offered, and then **b** (for Win95/FAT32).
   f. Verify the new partition configuration by entering **p**.

      Notice that a new hda7 partition has been added to the table.

4. Create 2 more logical partitions with the partition type of Linux (the default) by doing the following:
   a. Create a new partition by entering **n**; enter **l** (lower case L); then accept the default first cylinder by pressing **Enter**.
   b. Indicate the partition size by entering **+1G**.
   c. Create a new partition by entering **n**; enter **l** (lower case L); then accept the default first cylinder by pressing **Enter**.
   d. Indicate the partition size by entering **+2G**.
   e. Verify the new partition configuration by entering **p**.

      Notice that 2 new partitions have been added to the partition table.

5. Write the new partition table to your hard drive and exit fdisk by entering **w**.

6. View the current partition table used by the kernel by entering:

   cat /proc/partitions

7. To be able to access the new partitions, the kernel has to update its partition table stored in memory. Do one of the following:
   - Reboot the system by entering **reboot**.

- Have the kernel update its partition table by entering **partprobe**.

8. View again the partition table used by the kernel by entering:

   cat /proc/partitions

Part III: Manage File Systems from the Command Line

To manage file systems from the command line, do the following:

1. From the GNOME desktop, open a terminal window; then **su -** to root (password **novell**).
2. Create the following file systems (depending on your hardware use sda instead of hda in the following steps):
   a. Create a new FAT32 file system on /dev/hda7 and give it the label "data1" by entering the following (make sure you don't have a typo when specifying the device in the command; there won't be a warning message, the command is executed immediately):

      mkfs.msdos -n data1 /dev/hda7

      A message such as mkfs.msdos 2.11 (12 Mar 2005) confirms the file system creation.

   b. Create a new ext2 file system on /dev/hda8 with verbose output by entering the following (make sure you don't have a typo when specifying the device in the command; there won't be a warning message, the command is executed immediately):

      mkfs -t ext2 -v /dev/hda8

      Notice that by adding the option -v, you received extensive information about the new file system.

   c. Create a new Reiser file system on /dev/hda9 that is only 625 MB by entering the following:

      mkreiserfs /dev/hda9 160000

      A warning message appears indicating that all data will be lost on /dev/hda9.

d. Continue by entering **y**.

3. Create the directories **data1, data2** and **data3** under /export/ by using **mkdir -p /export/data{1,2,3}**.

4. Verify that the directories were created by entering **ls -l /export**.

5. As root, using an editor of your choice, for instance vi in a terminal window, add entries to the file **/etc/fstab** for the new file systems:

   a. Open the file /etc/fstab in an editor.

   b. At the end of the file fstab, add the following entries:

      /dev/hda7 /export/data1 vfat defaults 1 2
      /dev/hda8 /export/data2 ext2 defaults 1 2
      /dev/hda9 /export/data3 reiserfs defaults 1 2

      You must include an empty line at the end of the file, otherwise the mount command cannot read the file.

      These entries make sure that the hda7, hda8, and hda9 partitions are mounted when starting or rebooting the system.

   c. When you finish, save /etc/fstab (when using vi, press Esc, then enter :wq).

6. From the terminal window, mount all of the new file systems and re-read the /etc/fstab file by entering **mount -a**.

7. View the information about the mounted file systems by entering the following 3 commands:

   mount
   cat /proc/mounts

(End of Exercise)

Exercise 4-2 Manage File Systems from the Command Line

In this exercise you practice to manage file systems from the command line.

In the previous exercise, you created various partitions and file systems. If you used /dev/sda previously, replace /dev/hda***x*** by /dev/sda***x*** in this exercise as well.

In the first part of this exercise, you run e2fsck on the ext2 file system you created on /dev/hda5, which is mounted on /apps.

In the second part of the exercise, you convert the partition /dev/hda8 to an ext3 file system by adding a journal; also add the label /export/data2 to it.

Then resize the Reiser file system on /dev/hda9 to use the entire partition and not just 625 MB.

Detailed Steps to Complete this Exercise:

- Part I: Run e2fsck
- Part II: Customize the File Systems

Part I: Run e2fsck

To run e2fsck, do the following:

1. Unmount the file system on /dev/hda5 (or /dev/sda5, depending on your hardware) by entering **umount /apps**.
2. Verify that the file system is no longer mounted by entering **mount**.

   The /dev/hda5 partition is not displayed.
3. Start a file system check on hda5 running in verbose mode with an automatic response of yes to prompts by entering the following:

   e2fsck -f -y -v /dev/hda5

4. Mount the /apps file system again by entering **mount /apps**.
5. Verify that the file system is mounted by entering **mount**.

Part II: Customize the File Systems

To customize the file systems, do the following:

1. Modify the partition /dev/hda8:
   a. From the terminal window, umount /dev/hda8 and view details about the ext2 file system on /dev/hda8 by entering the following:

      umount /dev/hda8 ; dumpe2fs /dev/hda8 | more

      Notice the block size and the file system state.

   b. Give the ext2 file system the volume name /export/data2 while the file system is unmounted by entering the following:

      tune2fs -L /export/data2 /dev/hda8

      Naming a file system can be useful in system rescue situations when the /etc/fstab is not available. It is common practice to use this naming convention.

   c. Verify that the file system now has a volume name by entering **dumpe2fs /dev/hda8 | less**.
   d. Add a journal to the file system (making it an ext3 file system) by entering **tune2fs -j /dev/hda8**.
   e. Verify that the file system now contains a journal by entering **dumpe2fs /dev/hda8 | less**.
   f. Mount /dev/hda8 again by entering **mount /dev/hda8**.
   g. View information about the mounted file systems by entering **mount**.

      Notice that the file system is still mounted as an ext2 file system.

   h. Unmount the partition /dev/hda8 again by entering **umount /dev/hda8**.

i. Verify that the file system state is clean by entering **dumpe2fs /dev/hda8 | less**.

j. Edit the file /etc/fstab to change the file system type from ext2 to ext3, as in the following:

/dev/hda8 /export/data2 ***ext3*** defaults 1 2

Save the file.

k. From the command line, re-read /etc/fstab and mount the partition as an ext3 file system by entering **mount -a**.

l. Verify the change by entering **mount**.

m. Unmount the partition /dev/hda8 again by entering **umount /export/data2**.

n. Mount the partition as an ext2 file system manually by entering the following:

mount -t ext2 /dev/hda8 /export/data2

o. Verify that the file system is mounted without a journal (as an ext2 file system) by entering **mount**.

As you can see, ext3 is backward compatible with ext2.

p. Remount /dev/hda8 as an ext3 file system and verify the change by entering the following 3 commands:

umount /export/data2
mount -a
mount

2. Modify the partition /dev/hda9:

a. View the size of the partition /dev/hda9 by entering **df -h**.

b. Unmount dev/hda9
umount /export/data3.

c. While the partition is unmounted, add a label to the file system of /export/ data3 by entering the following:

reiserfstune -l /export/data3 /dev/hda9

d. Resize the partition to consume the entire partition by entering **resize_reiserfs /dev/hda9**.

When no size is specified, the file system is resized to use all available space on the partition. Increasing the size of the ReiserFS is also possible when the file system is mounted.

e. Remount the partition by entering **mount -a**.

f. View the size of the partition by entering **df -h**.

The size is no longer 625 MB, but should be 1 GB or more depending on the size of your partition.

g. Unmount the partition to run a file system check on it by entering **umount /export/data3**.

h. Run a check on the file system on /dev/hda9 by entering the following:

reiserfsck -y /dev/hda9

i. Remount all file systems by entering **mount -a**.

(End of Exercise)

Exercise 4-3 Create Logical Volumes

In this exercise, you learn how to administer LVM with YaST.

In the first part of this exercise, use YaST to create two physical volumes (PV) with a size of 1 GB each. Add them to a volume group (VG) named projects. Within the volume group, add two logical volumes named pilot (750MB) and production (750MB), to be mounted under /projects/pilot and /projects/production, respectively.

In the second part of the exercise, increase the size of the logical volume production to the maximum space available within the volume group.

Detailed Steps to Complete this Exercise:

- Part I: Create LVM Physical Volumes, a Volume Group, and Logical Volumes
- Part II: Resize an LVM Volume

Part I: Create LVM Physical Volumes, a Volume Group, and Logical Volumes

To create LVM Physical Volumes, a Volume Group, and Logical Volumes, do the following:

1. Start **YaST**, enter the root password (**novell**), and select **System > Partitioner**.

   Acknowledge the warning message by selecting **Yes**.

   The Expert Partitioner dialog appears.

2. Create a new LVM partition by doing the following:
   a. Select **Create**.
   b. Select **Do not format**; then select or enter the following:
      - File system ID: **0x8E Linux LVM**

- End (cylinder): **+1GB**

c. Save the partition definition by selecting **OK**.

3. Create another 1GB LVM partition by repeating step 2.

   You should now have two 1GB LVM partitions.

4. Select the **LVM** button and enter the following in the **Create a Volume Group** dialog:
   - Volume Group Name: **projects**
   - Physical Extent Size: **4M**
5. Continue by selecting **OK**.
6. Add each Linux LVM physical volume to the volume group projects by selecting each physical volume (such as **/dev/hda10**) and then selecting **Add Volume**. Then select **Next**.

   The **Logical Volume Manager: Logical Volumes** dialog appears.
7. Add a logical volume **pilot** within the projects volume group:

   a. Select **Add**.

      A **Create Logical Volume** dialog appears.

   b. Enter or select the following:
      - Format (file system): **Reiser**
      - Logical volume name: **pilot**
      - Size: **750 MB**
      - Mount Point: **/projects/pilot**

   c. Save the logical volume definition by selecting **OK**.
8. Add a logical volume **production** within the projects volume group:

   a. Select **Add**.

      A **Create Logical Volume dialog** appears.

   b. Enter or select the following:
      - Format (File system): **Reiser**
      - Logical volume name: **production**

- Size: **750 MB**
- Mount Point: **/projects/production**

c. Save the logical volume definition by selecting **OK**.

9. Save the changes by selecting **Next**.

   You are returned to the Expert Partitioner.

10. In the Expert Partitioner select **Apply**.

    A message appears; accept the changes by selecting **Finish**.

11. From a terminal window, **su -** to root (password **novell**).

12. View the new LVM file systems by entering the following:

    df -h

    Notice the size of these new file systems.

13. View the device names and mount locations by entering **cat /etc/fstab**.

Part II: Resize an LVM Volume

To resize a LVM Volume, do the following:

1. From the YaST Control Center, select **System > LVM**.

   The LVM dialog appears.

2. From the **Logical volumes** list select **/dev/projects/production**; then select **Edit**.

   The Edit Logical Volume dialog appears.

   Notice the volume size.

3. Select the **max** button.

   Notice that the size changes to the maximum space available.

4. Continue by selecting **OK**.

5. Save the changes by selecting **Finish**; then confirm the notification by selecting **OK**.

6. From the terminal window, view the new size of production by entering
   df -h.
7. Close all open windows.

(End of Exercise)

SECTION 5 Manage System Initialization

In this section of the workbook, you learn how to do the following:

- "Manage the Boot Loader" on 5-2

  In this exercise, you practice booting into a shell and modifying /boot/grub/menu.lst.

- "Manage Runlevels" on 5-4

  In this exercise, you practice configuring runlevels.

Exercise 5-1 Manage the Boot Loader

In this exercise, you practice booting into a shell and modifying /boot/grub/menu.lst.

Enter init=/bin/bash at the boot prompt, modify /boot/grub/menu.lst to require a password before kernel parameters can be modified, and test the new GRUB configuration.

Detailed Steps to Complete this Exercise:

1. From the terminal window, su to root (**su -**) with a password of **novell**.
2. Reboot by entering **init 6**.
3. When the boot menu is displayed, press the **Spacebar** to stop the timer.
4. In the Boot Options field type **init=/bin/bash**; then press **Enter**.
5. When the bash prompt appears, remount the root partition read-writable by entering

   mount -o remount,rw, sync /
6. Using vi, edit /boot/grub/menu.lst.

   Put a comment sign (#) in front of the line starting with gfxmenu.

   Add the following line beneath it:

   password secret
7. (Optional) To avoid having the password in cleartext in the configuration file, you can use an MD5-Hash instead. You can create and include it in the file with the following command within vi:

   Press Escape

   Type

   :r! echo -e “secret\nsecret” | grub-md5-crypt

and press enter.

There will be some lines of output from grub-md5-crypt in the file, including the MD5-hash of your password.

Delete the lines from the output of grub-md5-crypt except the line with the hash. If you still have the line with password ***secret*** in the file, delete it, too.

At the beginning of the line with the hash write password --md5, so that the line looks like the following:

password --md5 1t9kdK1$juAcBOwF18QFVf3Cl7b.v0

Note: Your hash value will be different than that given here.

Save the file by pressing **Esc** and **:wq**.

8. Mount the root file system read-only again:

   mount -o remount,ro /

   If the file system is mounted read-writable when you reset the computer in the next step, a file system check would need to be done when it starts up again.

9. Reset the computer.

   As you turned off the graphical menu, you will notice that the start screen looks different now.

10. If you want to edit the kernel command line, press **p** and then enter the password used in Step 6 or 7. A short help text informs you about the available options.

11. Press **b** to boot the computer.

12. Undo the changes in /boot/grub/menu.lst:

    a. Log in as geeko, open a terminal window, **su -** to root (password **novell**)

    b. Open /boot/grub/menu.lst with vi, put a comment sign at the beginning of the line starting with password. Save the file and close vi by pressing **Esc** and entering **:wq**.

(End of Exercise)

Exercise 5-2 Manage Runlevels

In this exercise, you practice configuring runlevels. This exercise has four parts.

In the first part, use the command runlevel to find out about the current runlevel and the command init to change to runlevel 3 and then back to 5.

In the second part, activate the **at** service atd. The service at allows commands to be scheduled at a future point in time.

In the third part, reboot your computer and boot into runlevel 3 instead of the default runlevel 5. Login and switch to runlevel 5.

In the fourth part, activate the rsync daemon using the YaST runlevel editor.

Detailed Steps to Complete this Exercise:

- Part I: View and Change the Current Runlevel
- Part II: Activate the at Service atd
- Part III: Set a Runlevel at Boot Time
- Part IV: Enable rsyncd with YaST

Part I: View and Change the Current Runlevel

To view and change the current runlevel, do the following:

1. Open a terminal window and **su -** to root (password **novell**).
2. Check the previous and current runlevels by entering **runlevel**.

   List the runlevels:

Table 5-1

Previous	Current

Notice that the previous runlevel is listed as N, which means that there was no previous runlevel set.

3. Change to runlevel 3 by entering **init 3**.

   The graphical environment is terminated and you are left at a terminal login prompt.

4. Log in as **root** with a password of **novell**.

5. Check the previous and current runlevel by entering **runlevel**.

   List the runlevels:

Table 5-2

Previous	Current

6. Switch to runlevel 5 by entering **init 5**.

   The GUI login screen appears.

7. Log in as **geeko** with a password of **novell**.

Part II: Activate the at Service atd

To activate the at service atd, do the following:

1. From the terminal window, su to root (**su -**) with a password of **novell**.

2. View the current runlevel configuration for atd by entering **chkconfig atd -l**.

   Notice that configuration is off for all runlevels.

3. Install the service to its predefined runlevels by entering **insserv -d atd**.

4. Check the modified runlevel configuration for at by entering **chkconfig atd -l**.

   Notice that the default configuration for at sets runlevels 2, 3, and 5 to on.

5. Change to the directory /etc/rc.d/rc3.d by entering **cd /etc/rc.d/rc3.d**.
6. List the atd files in the directory by entering **ls -l *atd**.

   Notice that there are two atd links—one is used to start and one is used to kill the service atd.
7. Start the service at by entering **rcatd start**.
8. Verify that the service is running by entering **rcatd status**.
9. Switch to virtual terminal 1 by pressing **Ctrl+Alt+F1**; then log in as **root**.
10. Switch to runlevel 1 by entering **init 1**.
11. Enter a root password of **novell**.
12. Check to see if the service is running by entering **rcatd status**.

    The service is listed as unused because it is not configured to start at runlevel 1.
13. Switch back to your previous runlevel (5) by entering **init 5**.

    The GUI login screen appears.
14. Log in as **geeko** with a password of **novell**.
15. Open a terminal window and **su -** to root (password **novell**).
16. Now use chkconfig instead of insserv to configure system services. From the command line, remove the service at from system startup runlevels by entering **chkconfig atd off**.
17. View the current runlevel configuration for at by entering **chkconfig atd -l**.

    Notice that the service is off for all runlevels.
18. Re-enable the service to start at the default runlevels by entering **chkconfig atd on**.

Part III: Set a Runlevel at Boot Time

To set a runlevel at boot time, do the following:

1. From the terminal window, su to root (**su -**) with a password of **novell**.
2. Reboot by entering **init 6**.
3. When the boot menu is displayed, press the **Spacebar** to stop the timer.
4. In the Boot Options field type **3**; then press **Enter** to boot the Linux system to runlevel 3.
5. When the login prompt appears, log in as **root** with a password of **novell**.
6. Display the current runlevel by entering **runlevel**.
7. Switch to runlevel 5 by entering **init 5**.
8. Switch back to the virtual terminal by pressing **Ctrl+Alt+F1**.
9. Log out as root by entering **exit**.
10. Switch back to the graphical user interface by pressing **Ctrl+Alt+F7**.
11. Log in as **geeko** with a password of **novell**.

Part IV: Enable rsyncd with YaST

To enable rsyncd with YaST, do the following:

1. From the graphical desktop, start **YaST**.

   The YaST Control Center appears.
2. Select **System > System Services (Runlevel)**.

   The Runlevel Editor: Services dialog appears.
3. Switch to a more detailed view (with additional options) by selecting **Expert Mode**.
4. Scroll down the Services list and select **rsyncd**.

5. Below the list, configure this service to start at runlevels 3 and 5 by selecting **3** and **5**.
6. From the Set/Reset drop-down list select **Enable the service**.
7. Start the service rsyncd from the Start/Stop/Refresh drop-down list by selecting **Start now**.

   A status message appears indicating that the service started successfully.
8. Close the status message by selecting **OK**.
9. Stop the service rsyncd from the Start/Stop/Refresh drop-down list by selecting **Stop now**.

   A status message appears indicating that the service stopped successfully.
10. Close the status message by selecting **OK**.
11. Save the changes by selecting **Finish**; then select **Yes**.
12. Close the YaST Control Center and the terminal window.

(End of Exercise)

SECTION 6 Configure Mail and Web Services

In this section of the workbook, you learn how to do the following:

- "Send Mail in the Local Network" on 6-2

  In this exercise, you send mail in the local network. You configure Postfix and test your configuration.

- "Use Postfix on the Internet" on 6-4

  In this exercise, you configure Postfix to send email to the Internet.

- "Use Lookup Tables" on 6-6

  In this exercise, you use the Postfix lookup tables.

- "Install Apache" on 6-9

  In this exercise, you install the apache components on your system.

- "Test the Apache Installation" on 6-10

  In this exercise, you check if the installation of apache was successful.

- "Configure a Virtual Host" on 6-11

  In this exercise, you configure a virtual host for the accounting department.

Exercise 6-1 Send Mail in the Local Network

In this exercise, you edit the Postfix configuration file /etc/postfix/main.cf. You configure Postfix to send mails in your local network. The domain name of the sender should be masqueraded for normal users. External mails should be forwarded to da1. Test your configuration by sending a mail to root.

Do the following:

- Part I - Edit /etc/postfix/main.cf
- Part II - Test the Configuration

Part I - Edit /etc/postfix/main.cf

1. Open a terminal window and enter **su-** to get root permissions.
2. When prompted, enter the root password **novell**.
3. Stop the postfix daemon by entering

   rcpostfix stop
4. Open the file /etc/postfix/main.cf in a text editor.
5. Scroll to the settings at the end of the file.
6. To accept mail only from the local network, edit the following options:
   - **inet_interfaces = *your_IP-Address*, 127.0.0.1**
   - **mynetworks_style = subnet** (should already be set)
   - **smtpd_recipient_restrictions = permit_mynetworks, reject** (on one line)
7. To rewrite the sender addresses and remove the host name, edit the following options:
   - **masquerade_exceptions = root** (should already be set)
   - **masquerade_domains = digitalairlines.com**

8. To deliver external mail to the relay host da1, edit the following option:

   relayhost = 10.0.0.254

9. Save the file and close the editor.

10. Start Postfix by entering

    rcpostfix start

Part II - Test the Configuration

1. To generate a test mail, do the following:
   a. Log out as user root by entering **exit**.
   b. Enter **mail root@*hostname*.digitalairlines.com**.

2. Enter the subject and some text and finish the mail by doing the following:
   a. Press **Enter**.
   b. Type **.** (dot).
   c. Press **Enter**.

3. Enter **su -** to get root permissions again.

4. When prompted, enter the root password **novell**.

5. Enter **mail**.

6. Enter the number corresponding to the mail you wrote.

7. Enter **q** to quit.

(End of Exercise)

Exercise 6-2 Use Postfix on the Internet

In this exercise, you configure Postfix to send email to the Internet. Only email from the local network should be allowed to accepted; any email that is not addressed to one of the local domains should be rejected.

Do the following:

1. Open a terminal window and enter **su-** to get root permissions.
2. When prompted, enter the root password **novell**.
3. Stop the postfix daemon by entering

   rcpostfix stop
4. Open the file /etc/postfix/main.cf with your favorite text editor.
5. To configure Postfix to accept email from the local network and email that is addressed to any recipient in the domain digitalairlines.com, edit or add the following options:
   - **myhostname = *hostname*.digitalairlines.com**
   - **mydomain = digitalairlines.com**
   - **mydestination = $myhostname, localhost.$mydomain, $mydomain** (on one line)
   - **smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination**

   The first three lines define hostnames and domains. The last line tells Postfix to accept mail as long it is sent from a host in mynetworks and to reject any mail that is not addressed to one of the domains defined in mydestination.
6. Save the file and close the editor.
7. Start Postfix by entering **rcpostfix start**.

(To test the configuration, you would have to access Postfix from an IP address outside the local network and try to send an email to a domain other than digitalairlines.com. Postfix should not accept this mail. However, the courseroom setup does not provide such a machine.)

(End of Exercise)

Exercise 6-3 Use Lookup Tables

In this exercise, you use the Postfix lookup tables.

In part I, you create a new user jgoldman with password novell.

In part II, you modify a lookup table that the email messages of a new user jgoldman are sent with the sender address webmaster@digitalairlines.com.

You test your configuration in part III.

Do the following:

- Part I - Create a New User jgoldman and Write an Email to root
- Part II - Change the sender_canonical Table and Write the Email Again
- Part III - Test the Configuration

Part I - Create a New User jgoldman and Write an Email to root

1. Open a terminal window and enter **su -** to get root permissions.
2. When prompted, enter the root password **novell**.
3. To create a new user jgoldman, enter
   useradd -G users -m jgoldman
4. Set the password for jgoldman to “novell” by entering
   passwd jgoldman

   Enter **novell** twice.
5. Log in as user jgoldman by entering
   su - jgoldman
6. To write an email to user root, enter
   mail root@localhost
7. Enter a subject and some text; then finish the email:
   a. Press **Enter**.
   b. Type **.** (dot).

c. Press **Enter**.

8. To get root permissions, enter **exit**.
9. Enter **mail**.
10. Enter the number corresponding to the email you just wrote.
11. Record the sender's address in the space below:

12. Enter **q** to quit.

Part II - Change the sender_canonical Table and Write the Email Again

1. Enter **rcpostfix stop**.
2. Open the file /etc/postfix/sender_canonical with your favorite text editor.
3. To change the sender address of user jgoldman, enter (on one line)
   jgoldman@da*xx*.digitalairlines.com webmaster@digitalairlines.com
4. Save the file and close the editor.
5. Enter **postmap hash:/etc/postfix/sender_canonical**.
6. Start Postfix by entering
   rcpostfix start

Part III - Test the Configuration

1. Log in as user jgoldman by entering
   su - jgoldman
2. To write an email to user root, enter
   mail root@localhost

3. Enter a subject and some text; then finish the email:
   a. Press **Enter**.
   b. Type **.** (dot).
   c. Press **Enter**.
4. To get root permissions, enter **exit**.
5. Enter **mail**.
6. Enter the number corresponding to the email you just wrote.
7. Record the sender's address in the space below:

8. Enter **q** to quit.

(End of Exercise)

Exercise 6-4 Install Apache

In this exercise, you install the apache components on your system.

Do the following:

1. Start YaST.
2. From the YaST Control Center, select **Software > Software Management**.
3. From the filter drop-down menu, select **Search**.
4. In the Search field, enter **apache**; then select **Search**.
5. On the right side, select the following packages.
   - **apache2**
   - **apache2-example-pages**
   - **apache2-prefork**
6. Select **Accept**.
7. (Conditional) If YaST displays package dependencies, confirm by selecting **Continue**.
8. When prompted, insert the requested SUSE Linux Enterprise Server 10 CDs in the drive.
9. When installation is complete, close the YaST Control Center and remove the CD.
10. Open a terminal window and su to **root**.
11. To start Apache at boot time, enter the following:

    insserv apache2
12. To start the Apache daemon, enter the following:

    rcapache2 start

(End of Exercise)

Exercise 6-5 Test the Apache Installation

In this exercise, you check if the installation of apache was successful.

Do the following:

1. Start Firefox.
2. In the address bar of the web browser, enter the following:

   http://localhost

   If the Apache example page appears, the web server has been installed and started correctly.
3. (Conditional) If you are having problems displaying the page, you need to rename the file /srv/www/htdocs/index.html.en to **/srv/www/htdocs/index.html**.

(End of Exercise)

Exercise 6-6 Configure a Virtual Host

In this exercise, you configure a virtual host for the accounting department.

The file **accounting.conf** you create in this exercise can be difficult to modify properly. To help you understand what needs to be changed and where parameters are placed, the file is available on your *3073 Course CD* in the directory **/exercises/section_2**.

Do the following:

1. From the terminal window (as root), create a directory for the virtual host by entering the following:

   mkdir /srv/www/accounting

2. In the new directory, create a file **index.html** with the following content:

```
<html>
 <head>
  <title>Accounting Intranet Server</title>
 </head>
 <body>
  <h1>Accounting Intranet</h1>
  Under construction.
 </body>
</html>
```

This file is also available on your *3073 Course CD* in the directory **/exercises/section_2**.

3. Change to the directory /etc/apache2/vhosts.d/ by entering the following:

   cd /etc/apache2/vhosts.d/

4. Copy the virtual host template file by entering the following:

   cp vhost.template accounting.conf

5. Open the file **accounting.conf** in a text editor and make the following changes:

   <VirtualHost accounting.da.com:80>

   ServerName accounting.da.com

   DocumentRoot /srv/www/accounting

   ErrorLog /var/log/apache2/accounting.da.com-error_log

   CustomLog /var/log/apache2/accounting.da.com-access_log combined

   UseCanonicalName On

   ScriptAlias /cgi-bin/ "/srv/www/cgi-bin"

   <Directory "/srv/www/cgi-bin">
   AllowOverride None
   Options +ExecCGI -Includes
   Order allow,deny
   Allow from all
   </Directory>

   <Directory "/srv/www/accounting/">
   AllowOverride None
   Options Indexes FollowSymLinks
   Order allow,deny
   Allow from all
   </Directory>

6. For testing purposes, append "accounting.da.com" to the line "127.0.0.1" in the file **/etc/hosts**:

   127.0.0.1 localhost accounting.da.com

7. Test the syntax of your configuration file by entering the following:

   apache2ctl configtest

8. Reload Apache by entering the following:

   rcapache2 reload

9. From the Konqueror browser, access the virtual host by entering the following:

   http://accounting.da.com

   The accounting intranet index page is displayed.

10. Close the Konqueror browser.

(End of Exercise)

SECTION 7 AppArmor

In this section of the workbook, you learn how to do the following:

- "AppArmor" on 7-2

  In this exercise, you create, test, and improve a profile for the Firefox browser.

Exercise 7-1 AppArmor

In this exercise, you create, test, and improve a profile for the Firefox browser. This exercise has four parts.

In the first part create a profile for the Firefox browser. While using Firefox to generate log entries for the initial profile, just surf the web; do not access local files with Firefox.

In the second part, use Firefox to access a local file, such as /usr/share/doc/packages/apparmor-docs/apparmor.7.html. AppArmor should prevent you from viewing the file. Change the profile to allow access. You could use YaST, genprof, or complain and logprof for this purpose.

In the third part, install the Java browser plug-in package java-1_4_2-sun-plugin. Restart Firefox and use it to access a page containing a Java applet.

http://java.sun.com/products/plugin/1.4/demos/plugin/applets.html links to various demos. Firefox will not be able to show these. Change the profile again to be able to run Java applets. Use another method to do so than the method used in part two above.

In the fourth part, compare the profile you generated with those in /etc/apparmor/profiles/extras/ for Firefox. Find out if your profile is more restrictive or more permissive compared with those profiles.

Detailed Steps to Complete this Exercise

- Part I: Create a Profile for the Firefox Browser
- Part II: Modify the Profile for Firefox to Allow Read Access to the Local File System
- Part III: Use a Browser Plug-in
- Part IV: Compare the Profile You Created with Those From SLES 10

Part I: Create a Profile for the Firefox Browser

Do the following:

1. Start **Yast**, enter the root password (**novell**).
2. Select **Novell AppArmor > Add Profile Wizard**.
3. At the prompt: **Application to Profile**, enter **firefox**.
4. Start Firefox by pressing **Alt+F2**, entering **firefox** and selecting **Run**. View some web pages. Close Firefox again.
5. In the YaST AppArmor Profile Wizard dialog, select **Scan system log for AppArmor events**.
6. Now you create the profile and need to answer several questions. Note that the application Firefox is quite complex and accesses several executables and files on the system.
   a. Select **Inherit** for /bin/basename and other executed program .
   b. For files and directories, choose an appropriate option, such as an #include, a filename, a directory, or a path with place holders, and select **Allow**.
7. When you are returned to the AppArmor Profile Wizard dialog, select **Finish**.
8. Make sure that the Firefox profile is in enforce mode by looking at **/sys/kernel/security/apparmor/profiles** using cat. There must be an entry **/usr/lib/firefox/firefox.sh (enforce)**. If it is not, execute **enforce firefox**.

Part II: Modify the Profile for Firefox to Allow Read Access to the Local File System

Do the following:

1. Open a terminal window and su - to root (password **novell**).
2. Enter **tail -f /var/log/audit/audit.log**.
3. Start Firefox by pressing **Alt+F2**, entering **firefox** and selecting **Run**. Try to view the file /usr/share/doc/packages/apparmor-docs/apparmor.7.html. (You should not be able to do so.)
4. View the log file in the terminal window. You should see a reject message.
5. Stop viewing the log file by pressing **Ctrl+c**.
6. In the terminal window, enter **complain firefox**.
7. In Firefox, try again to access /usr/share/doc/packages/apparmor-docs/apparmor.7.html. You should now be able to access the file.
8. Start **Yast**, enter the root password (**novell**).
9. Select **Novell AppArmor > Update Profile Wizard**.
10. You are presented with the same interface as in Part I, where you can choose Allow, Inherit, Deny, etc. Make sure you are updating the Firefox profile, not some other profile.

    Sooner or later you should see an entry for the path /usr/share/doc/packages/apparmor-docs/apparmor.7.html. By selecting the Glob button three times, you can create a suggestion /usr/share/doc/**. Allow it by selecting Allow.
11. When all entries in the log file have been processed, select **Finish**.
12. Put the Firefox profile back in enforce mode by entering **enforce firefox** in the terminal window.

13. In Firefox, try to access files beneath /usr/share/doc/, like /usr/share/doc/packages/. You should be able to access them. However, accessing files elsewhere in the file system should not be possible.
14. Close Firefox.
15. Close YaST.

Part III: Use a Browser Plug-in

Do the following:

1. Open a terminal window and **su -** to root (password **novell**).
2. Install the Java Browser Plug-in by entering (as root):

   yast -i java-1_4_2-sun-plugin

   Insert the appropriate media when prompted. Do not close the console window after the installation.
3. Start Firefox by pressing **Alt+F2**, entering **firefox** and selecting **Run**.
4. Visit http://java.sun.com/products/plugin/1.4/demos/plugin/applets.html and select one of the demos. (The demo should not work.)
5. In the console window, enter

   genprof firefox

   When asked to exercise the functionality of your application, select one of the demos again as in the previous step. The demo should work now.
6. Close Firefox.
7. Go back to the console window and press **s** to scan the logfile. Select **i** for inherit when the entry for java_vm is shown.
8. Answer the subsequent questions with **Glob** and **Accept**, as applicable.
9. When all questions have been answered, press **f** to finish.

10. Start Firefox again and select another Java demo available at the URL given in Step 4. This should work now, despite the profile being in enforce mode again.

Part IV: Compare the Profile You Created with Those From SLES 10

Do the following:

1. Open a console window and view the profile /etc/apparmor.d/usr.lib.firefox.firefox.sh just created with cat.
2. Open another console window and view the profiles /etc/apparmor/profiles/extras/usr.lib.firefox.firefox*, using cat.
3. Compare the files. Note any differences and decide whether or not they are more restrictive than the one you created.

(End of Exercise)

SECTION 8 Manage Virtualization with Xen

In this section of the workbook, you learn how to do the following:

- "Install Xen" on 8-2

  In this exercise, you learn how to install Xen and configure domain0.

- "Install a Guest Domain" on 8-4

  In this exercise, you learn how to install a Xen guest domain using YaST.

- "Change Memory Allocation of a Guest Domain" on 8-6

  In this exercise, you learn how to change the memory allocation of a guest domain by changing the domain configuration file.

- "Check the Network Configuration" on 8-9

  This exercise assumes that you have a Xen system with domain0 and one more Xen domain running.

- "Automate Domain Startup" on 8-8

  In this exercise, you learn how to startup domains automatically when the system is booted.

Exercise 8-1 Install Xen

In this exercise, you learn how to install Xen and configure domain0.

Do the following:

- Part I: Install XenPackages.
- Part II: Prepare for Reboot
- Part III: Reboot and Test Xen.

Part I: Install XenPackages.

Do the following:

1. Start the **YaST Controll Center**.
2. Select **Software > Software Management**.
3. From the Filter menu, select **Search**.
4. Enter **xen** in the search field and select **search**.
5. On the right side, select the packages **xen**, **kernel-xen** and **xen-tools**.
6. Select **Accept** and let YaST install all required software packages.
7. **Close** the YaST Control Center.

Part II: Prepare for Reboot

Do the following:

1. Open a terminal window and **su -** to the root user.
2. Open the file **/boot/grub/menu.lst** with a text editor (eg. vi).
3. Make sure, that there is a section with the title **Xen** in the file.
4. In this section, make sure that the parameter **root=** points to the root partition of your installation.

5. Close the file.
6. Enter the command:
   insserv -r SuSEfirewall2_setup
   and
   insserv -r SuSEfirewall2_init
7. Close the terminal window.

Part III: Reboot and Test Xen.

1. Reboot your system.
2. At the boot menu, select the **Xen entry** and hit **Return**.
3. When the system has been booted, log in as user **geeko** with the password **novell**.
4. Open a terminal window and **su -** to the **root** user.
5. Enter the command **xm list**.
6. In the output you should see one domain (Domain-0) with the status running.

(End of Exercise)

Exercise 8-2 Install a Guest Domain

In this exercise, you learn how to install a Xen guest domain using YaST. Before you start with this exercise ,you must have installed xen on your system.

Do the following:

1. Open the **YaST Control Center**.
2. Select **System > Virtual Machine Management**.
3. Select **Add**.
4. Select **Run an OS installation program** and then **Next**.
5. Select **Next**.
6. After a while, a terminal window opens and a standard SUSE Linux Enterprise Server installation starts up. Select this window.
7. Press **Alt+N**.
8. Use the tab-key to navigate to the item "**Yes, I Agree to the License Agreement**". Then press the space bar.
9. Press **Alt+N.**
10. Press **Alt+N**.
11. (Optional) Adjust the settings for **Region** and **Time Zone**. Navigate to the menus with the tab-key and use the arrow keys to change an option.
12. Press **Alt+N**.
13. Confirm the installation overview by pressing **Alt+A**.
14. Start the installation by pressing **Alt+I**.
15. (Wait till the installation has been finished.)
16. Select **Continue** in the **Installation Complete** message box.
17. Select **Next** in the domain configuration overview.
18. Select **Finish** in the **Virtual Machine Started** message box.
19. Switch to the terminal of the virtual domain.

20. Select **Next** (Press **Alt+P**).
21. Enter **novell** as root password. Select **Next** to continue (Press **Alt+N**).
22. Accept that the password is too simple.
23. Select **Alt-n** to continue.
24. Select **No, Skip this Test** (Press **Alt+O**).
25. Select **Next** (**Alt+N**).
26. Select **Next** (**Alt+N**).
27. Select **Next** (**Alt+N**).
28. Create user **geeko** with the password **novell**.
29. Select **Next** (**Alt+N**).
30. Accept that the password is too simple.
31. Select **Next** (**Alt+N**).
32. Select **Next** (**Alt+N**).
33. Select **Finish** (**Alt+F**).
34. Test if you can login to the new domain as the user root with the password novell.
35. Please do not close the terminal window, we will use it in the next exercise.

(End of Exercise)

Exercise 8-3 Change Memory Allocation of a Guest Domain

In this exercise, you learn how to change the memory allocation of a guest domain by changing the domain configuration file.

The following assumes, that you still have an open terminal window of the guest domain, that you have configured in the previous exercises.

Do the following:

1. Open a terminal window and **su -** to the root user.
2. Enter the command **xm list**.
3. Note the memory allocation of the domain vm1.
4. Switch to the terminal of the Xen domain and halt the system by typing **halt**. Wait till the system has been halted.
5. Return to the root terminal and use the command xm list to verify that the domain vm1 is not running anymore.
6. Open the file **/etc/xen/vm/vm1** with a text editor.
7. Look for the **memory** parameter and change the value to **172**.
8. Save and close the file.
9. Enter the following command to start the domain:

   xm create -c -f /etc/xen/vm/vm1
10. Wait till the system has been booted and you see the login prompt.
11. Press the key combination **Ctrl-]** to detach from the domain terminal and return to the root terminal.
12. Use the command **xm list** to determine the memory allocation of domain vm1. It should be 172MB.
13. Also note the **ID** of domain vm1.

14. Attach to the terminal of vm1 with the command **xm console <noted_id>**

(End of Exercise)

Exercise 8-4 Automate Domain Startup

In this exercise, you learn how to startup domains automatically when the system is booted.

Do the following:

1. Open a terminal window and **su -** to the root user.
2. Move the vm1 configuration file into the auto directory: **mv /etc/xen/vm/vm1 /etc/xen/auto/**
3. Shutdown vm1 with the command **xm shutdown vm1.**
4. Wait a moment and control with the command **xm list** if the domain has been shut down. Continue with next step when the domain vm1 is not listed anymore.
5. Reboot you system by entering **reboot**.
6. At the boot prompt, select the **Xen** entry.
7. When the system has been started up, log in to the graphical interface as user geeko with the password novell.
8. Open a terminal window and **su -** to the root user.
9. Enter the command **xm list**.
10. The domain vm1 should have been automatically started and should be listed in the xm output.

(End of Exercise)

Exercise 8-5 Check the Network Configuration

This exercise assumes that you have a Xen system with domain 0 and one more Xen domain running.

Do the following:

1. Open a terminal window and **su -** to the root user.
2. Make sure that the domain vm1 is running by typing the command **xm list**.
3. In the output of the xm command, note the **ID** of the domain vm1.
4. View the network bridge configuration with the command **brctl show.**
5. You should see the configuration of the bridge xenbr0. The interfaces **peth0** (physical interface) **vif0.0** (virtual interface of domain 0) and the virtual interface **vifx.0** (where x is the domain ID of domain vm1) should be added to the bridge.
6. Shutdown the domain with the command **xm shutdown vm1**.
7. Wait a moment and control with the command **xm list** if the domain has been shut down. Continue with next step when the domain vm1 is not listed anymore.
8. Enter the command **brctl show** again. Note that the inerface of the domain vm1 has been removed from the bridge.
9. Restart the domain with: **xm create -f /etc/xen/vm/vm1**
10. Note the ID of **vm1** and check with **brctl show** if the interface of vm1 has been added again.

(End of Exercise)

SECTION 9 iSCSI

In this section of the workbook, you learn how to do the following:

- "Set up an iSCSI Target and an iSCSI initiator" on 9-2

  In this exercise, you set up iSCSI.

Exercise 9-1 Set up an iSCSI Target and an iSCSI initiator

In this exercise, you learn how to set up an iSCSI target and how to access that target using an iSCSI initiator.

In part 1, set up an iSCSI target on your machine.

In part 2, set up an iSCSI initiator that accesses the iSCSI target on your own machine.

In part 3, you work with another student. Set up an iSCSI initiator on of your machines that connects to the iSCSI target on the other machine instead of localhost as configured in Part II

Part I: Set up an iSCSI target on your machine

1. Install the needed packages with the command:

   yast -i iscsitarget open-iscsi

2. Create an empty file with a size of 1GB used as backend storage:

   dd if=/dev/zero of=/srv/iscsi/ocfs2_disk.img bs=1M count=1024

3. Open the YaST iSCSI target module by starting **YaST** and selecting **Network Services > iSCSI Target**.

4. On the Service tab, select **When Booting** within the **Service Start** section.

5. Leave the **Global** tab unchanged.

6. On the Targets tab, delete the existing target, then select new and enter:

   Target: **iqn.*yyyy-mm*.com.digitalairlines.*daxx***

   Identifier: **storage.disk1**

   Lun: **0**

   Path: **/srv/iscsi/ocfs2_disk.img**

   Select **Next**.

7. In the authentication dialog, select **Incoming Authentication > Add**; enter ***root*** as username and ***novell*** as password.

   Select **Next**. You are returned to the iSCSI Target Overview dialog.

8. Close the dialog by selecting Finish.

9. In a terminal window, check the file /etc/ietd.conf. It should look similar to the following:

```
Target
iqn.2006-10.com.digitalairlines.da3:storage.disk1
Lun 0 Path=/srv/iscsi/ocfs2-disk.img,Type=fileio
IncomingUser root novell
        # Users, who can access this target.
...
```

Part II: Set up an iSCSI Initiator Connecting to the iSCSI Target on Your Host.

1. View the content of the directory /dev/disk/by-path/ using **ls**.

2. Open the YaST iSCSI initiator module by starting **YaST** and selecting **Network Services > iSCSI Initiator**.

3. On the Service tab, select **When Booting** within the **Service Start** section.

4. On the **Discovered Targets** tab, select **Discovery**. Fill in the iSCSI Discovery Dialog:

   IP Address: **127.0.0.1**

   Select Outgoing Authentication

   Username: **root**

   Password: **novell**

5. Select the discovered target, then select **Log In**. Enter Username and Password again as needed.

6. On the Connected Targets tab, check that the storage is available and toggle start-up to automatic by selecting **Toggle Start-Up**.

7. Leave YaST and check if the device appeared in /dev/disk/by-path/ using ls.

Part III: Set up an iSCSI Initiator Connecting to an iSCSI Target on Another Host.

During this part you have to work with another student.

1. Decide who of you is going to change his configuration from Part II. The other one will leave his configuration unchanged.
2. On the computer where you are going to change the configuration, open the YaST iSCSI initiator module by starting **YaST** and selecting **Network Services > iSCSI Initiator**.
3. On the Service tab, select **When Booting** within the **Service Start** section as in Part II.
4. On the **Connected Targets** tab, select **Log Out**; confirm the warning by selecting **Continue**.
5. On the **Discovered Targets** tab, select Delete. Then select **Discovery**. Fill in the iSCSI Discovery Dialog:

   IP Address: ***IP_Address_of_partners_computer***

   Select Outgoing Authentication

   Username: **root**

   Password: **novell**
6. Select the discovered target, then select **Log In**. Enter Username and Password again as needed.
7. On the **Connected Targets** tab, check that the storage is available and toggle start-up to automatic by selecting **Toggle Start-Up**.
8. Leave YaST and check if the device appeared in /dev/disk/by-path/ using ls.
9. Reboot the other machine, then this one to see if all services are started correctly again.

You will use this device in the next Exercise.

(End of Exercise)

SECTION 10 Cluster File Systems

In this section of the workbook, you learn how to do the following:

- "Set up an OCFS2" on 10-2

  In this exercise, you set up OCSF2.

Exercise 10-1 Set up an OCFS2

This exercise builds on the previous one, "Set up an iSCSI Target and an iSCSI initiator" on page 9-2.

You continue to work with the partner from Part III of that exercise.

The purpose of this exercise is to familiarize you with OCFS2. For a production environment you would most probably want some failover capacity (for instance by using DRBD and Heartbeat); this is not covered in this course.

In this exercise, you set up an OCFS2 on top of the devices provided by iSCSI as configured in the previous exercise.

1. On both computers, install the needed packages with the command:

   yast -i ocfs-tools ocfs2console

2. On both computers, create an /etc/ocfs2/cluster.conf with the following content:

```
cluster:
     name = mycluster
     node_count = 2
node:
     name = daxx.digitalairlines.com
     cluster = mycluster
     number = 0
     ip_address = 10.0.0.xx
     ip_port = 7777
node:
     name = dayy.digitalairlines.com
     cluster = mycluster
     number = 1
     ip_address = 10.0.0.yy
     ip_port = 7777
```

   Replace xx by the number of the machine running the iSCSI target, yy for the other one.

3. On both computers, configure the OCSF2 cluster services, using the command:

   /etc/init.d/o2cb configure

   Answer the questions appropriately.

4. On the machine providing the iSCSI target, create an OCFS2 file system, using the command:

   mkfs.ocfs2 -b 4k -C 128k -N 4 -L mycluster /dev/sd*x*

   Replace sdx by the proper device.

5. Create a directory /ocfs-cluster-fs

6. On both machines, create an entry in /etc/fstab for the file system, adding a line similar to the following to the existing entries:

   /dev/sdb /ocfs-cluster-fs ocfs2 defaults 0 0

7. On both machines, mount the file system by entering

   rcocfs2 start

   Check if the file system has been mounted using the command mount.

8. On one machine create a file in /ocfs-cluster-fs; it should appear be visible in the other system.

(End of Exercise)